



HECHO EN CHINA , DESHECHO EN ESPAÑA

DIEZ AÑOS FORTALECIENDO LA
CIBERSEGURIDAD NACIONAL

HECHO EN CHINA ,
DESHECHO EN ESPAÑA

- Francisco Lázaro Anguís
- Renfe
- flazaro@renfe.es

renfe

HECHO EN CHINA, DESHECHO EN ESPAÑA.

Objetivo de la Ponencia.

- Evidenciar el gran nivel de las compañías, servicios, herramientas y profesionales españoles.
- Poner de manifiesto el efecto positivo de la colaboración entre Organismos y empresas Españolas.
- Mostrar el uso cooperativo de esos servicios, herramientas, profesionales , españoles, así como de los recursos de colaboración, a través un caso (la Gestión de un incidente de seguridad).

Índice

1. Evolución del Sistema de Seguridad de la Información.
2. Recursos del Sistema de Seguridad de la Información.
3. Caso de estudio.

Seguridad TIC

- Estrategia, Políticas y Normas de Seguridad
- Gestión del Riesgo tecnológico
- Auditorías técnicas ,pruebas de penetración y gestión de vulnerabilidades
- Gestión de Incidentes de Seguridad
- Concienciación y Colaboración con terceros

Infraestructura de Seguridad

- Administración y Operación de la Infraestructura

Evolución del Sistema de Seguridad de la Información

Desde “La Seguridad de la Información” a “La Ciberseguridad.”



Incidentes

Especialización

Colaboración



Concienciación



Inteligencia

Proyectos

Evolución del Sistema de Seguridad de la Información

Desde “La Seguridad de la Información” a “La Ciberseguridad.”

- La especialización de recursos en incidentes de seguridad.
- El reporte de incidentes de seguridad a Organismos de Control.
- La necesidad de “industrializar” la defensa (ej: IOCs, tener modelado el proceso de reacción y contramedidas a los principales Incidentes de Seguridad).
- La intensificación de la colaboración (en cualquiera de las combinaciones publica/privada).
- Participación en Ciberejercicios para el continuo entranamiento en las capacidades de reacción ante Incidentes de Seguridad capaces de comprometer una organización.
- De Información a Inteligencia Operacional: Detección de Comportamientos, Data Analytics, Inteligencia Colectiva, IOCs, OSINT
- La modelización de las identidades y las entidades.

Evolución del Sistema de Seguridad de la Información

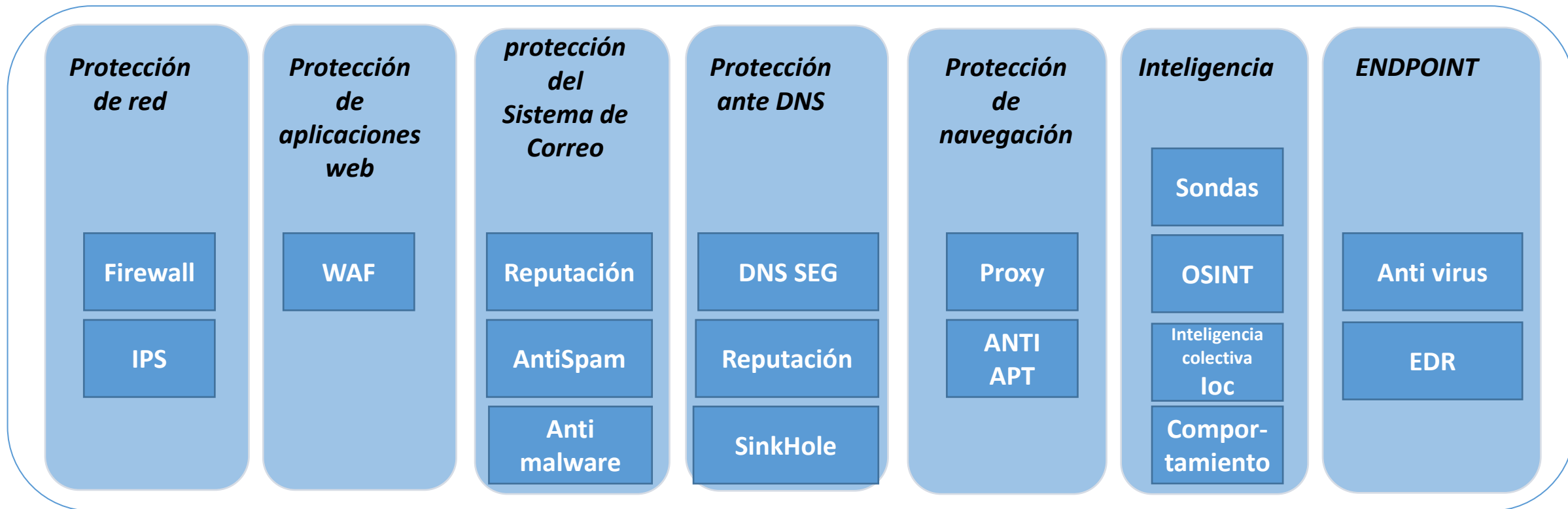
Desde “La Seguridad de la Información” a “La Ciberseguridad.”

- La retroalimentación de la gestión de riesgos con los incidentes de seguridad, la gestión de vulnerabilidades y las auditorías.

La mejora de los procesos y el acometimiento de proyectos remediadores/mitigadores.

- El incremento de la necesidad de concienciar.
- El incremento de la necesidad de comunicar avances y acciones.

RECURSOS DEL SISTEMA DE SEGURIDAD.



Siem

CERT

OFICINA DE PROYECTOS

CASO DE ESTUDIO

El comienzo...

- Estimado/a Sr/a.,

Desde el Sistema de Alerta Temprana de las Sondas de Internet nos ponemos en contacto con usted para informar sobre la siguiente alarma producida en nuestros sistemas, cuyo nivel de alerta está considerado como ALTO.

A continuación le informamos sobre la alarma producida en nuestros sistemas:

- 1) Evento
- 2) Información Detallada
- 3) Análisis del Evento
- 4) Análisis de IPs / Dominios
- 5) Recomendaciones
- 6) Reglas de Snort

1) EVENTO

Detectado posible rootkit ZeroAccess - Renfe

2) INFORMACIÓN DETALLADA

Se han detectado varias comunicaciones que indican una posible instalación de código dañino dentro de algunas máquinas de su organismo.

Los últimos eventos detectados son:

(2016-09-30 09:55:18) 213.144.48.176:49152 -> 221.194.47.208:53
(2016-09-30 09:55:17) 213.144.48.176:49152 -> 221.194.47.224:53
(2016-09-30 09:55:15) 213.144.48.176:49152 -> 221.194.47.224:53
(2016-09-30 09:55:07) 213.144.48.176:49152 -> 221.194.44.224:53
(2016-09-30 09:55:07) 213.144.48.176:49152 -> 221.194.44.224:53
(2016-09-30 09:54:58) 213.144.48.176:49152 -> 221.194.47.216:53
(2016-09-30 09:54:53) 213.144.48.176:49152 -> 221.194.44.224:53
(2016-09-30 09:54:52) 213.144.48.176:49152 -> 221.194.47.224:53
(2016-09-30 09:54:49) 213.144.48.176:49152 -> 221.194.47.224:53
(2016-09-30 09:54:46) 213.144.48.176:49152 -> 221.194.44.224:53
(2016-09-30 09:54:45) 213.144.48.176:49152 -> 221.194.47.208:53
(2016-09-30 09:54:44) 213.144.48.176:49152 -> 221.194.44.224:53

La lista de direcciones IP del organismo es:

* 213.144.48.176

La lista de direcciones IP implicadas es:

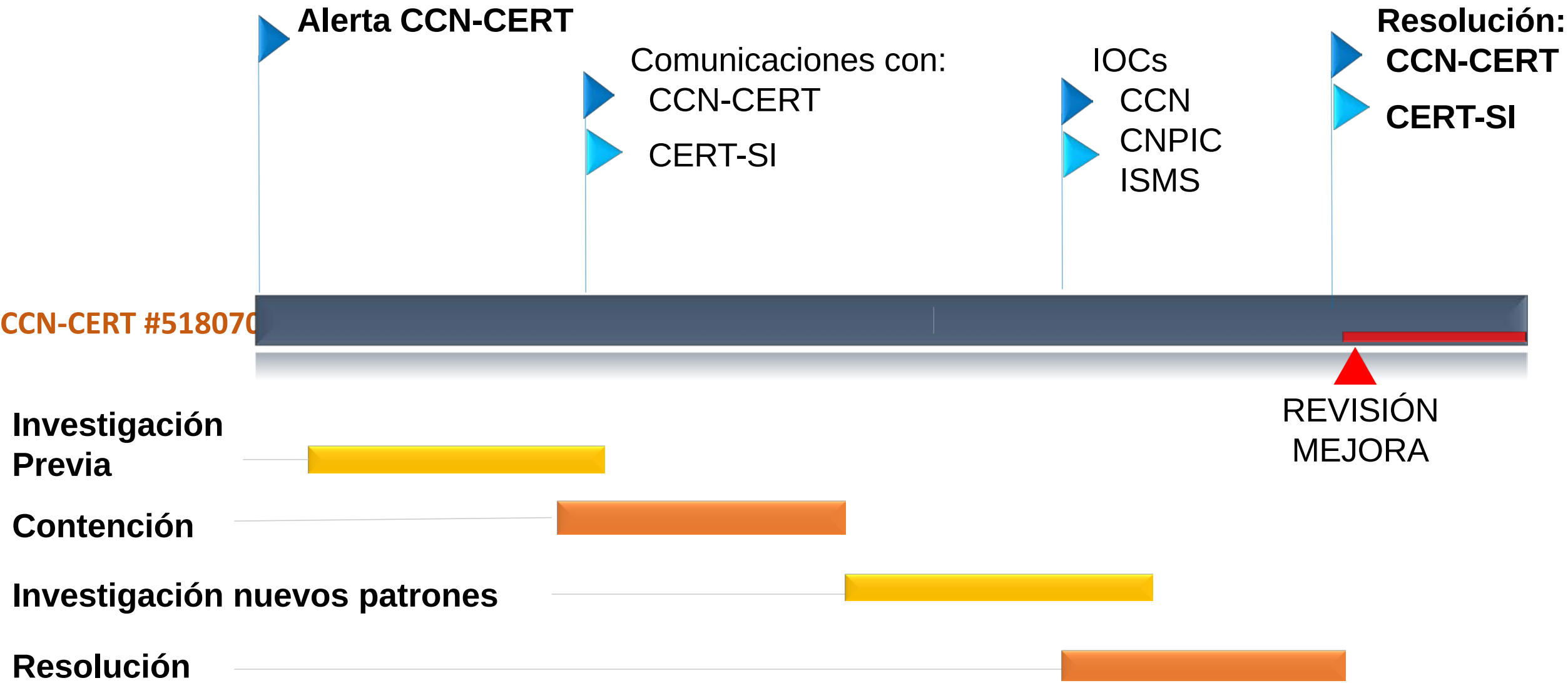
221.194.44.224 [China] China Unicom Hebei Province Network
221.194.47.208 [China] China Unicom Hebei Province Network
221.194.47.224 [China] China Unicom Hebei Province Network

3) ANÁLISIS DEL EVENTO

Las reglas en cuestión detectan paquetes con un patrón determinado de bytes. Este patrón está relacionado con el rootkit ZeroAccess [2, 3].

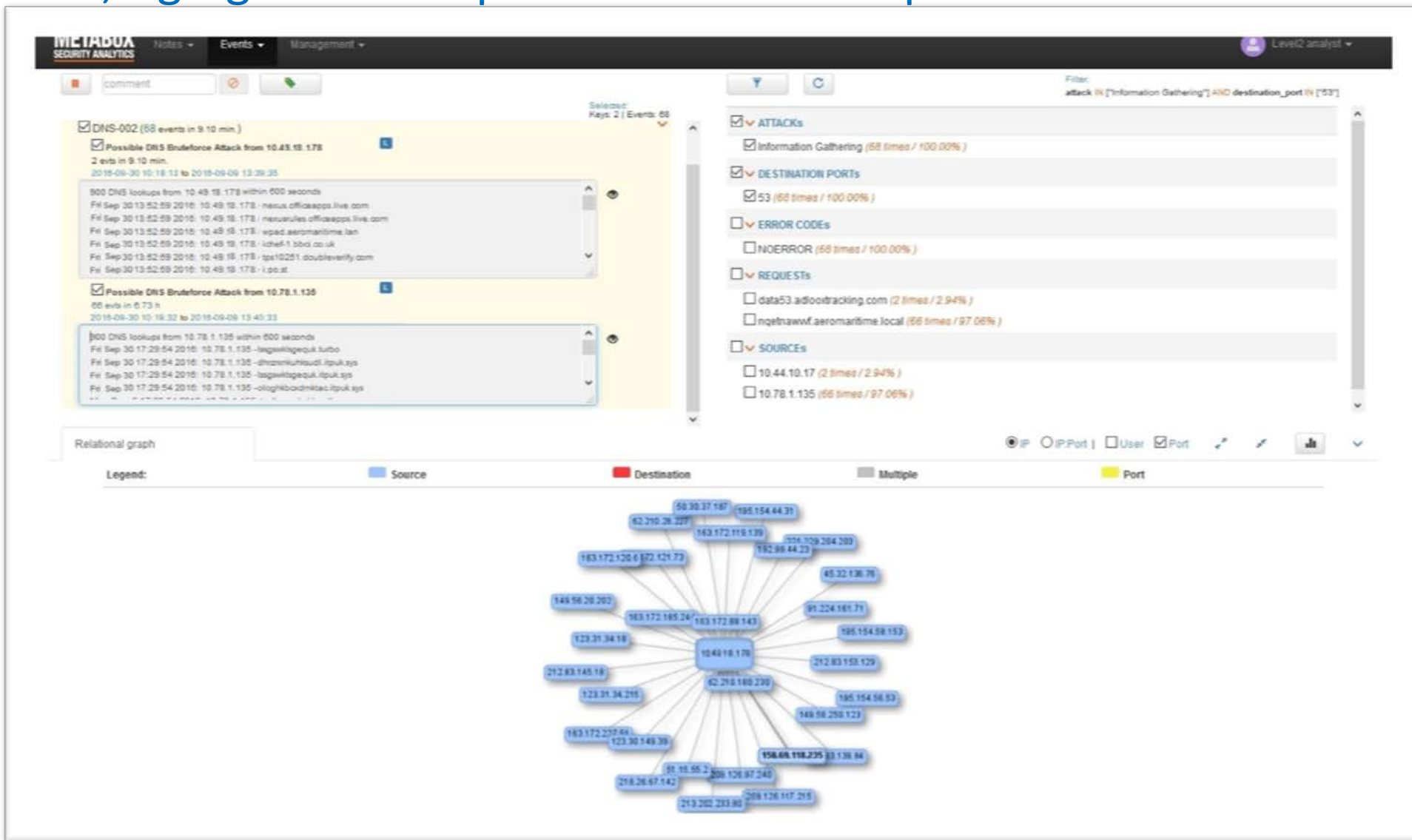
Este software está catalogado como troyano/rootkit, y tiene las siguientes características:

- * Crea un volumen oculto en el disco utilizando APIs de bajo nivel en el sistema.
- * Modifica drivers del sistema para inyectar código dañino a nivel de núcleo.
- * Sistemas para evitar la detección de antivirus y dificultar análisis forense.
- * Abre una puerta trasera en el sistema y que permite descargar y ejecutar otros códigos dañinos.
- * Monitorización de actividades del usuario mediante llamadas a procedimiento remoto asíncronas.

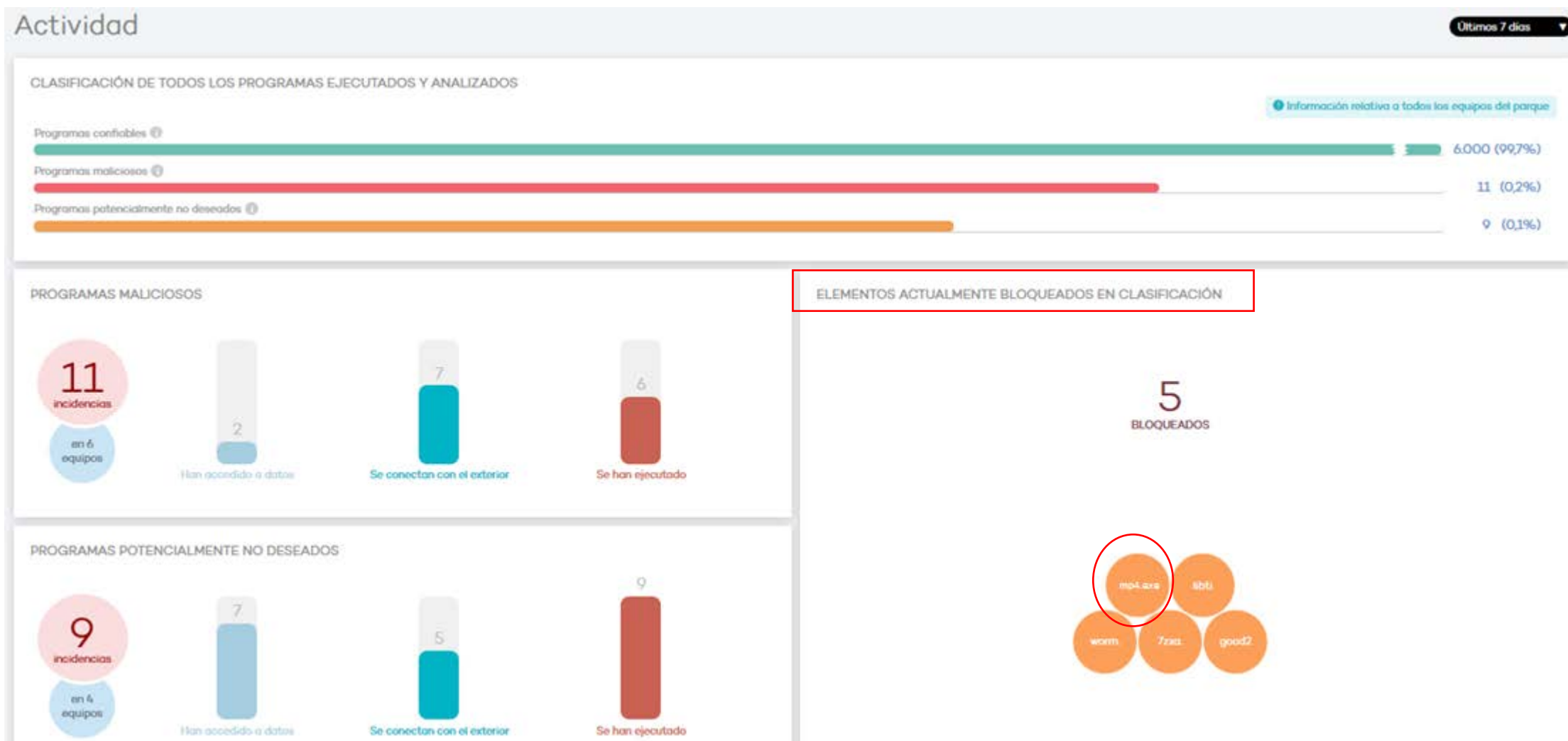


Metabox

Correlación, Agregación enriquecimiento en tiempo real



Adaptive Defense - Detección de Ejecutables Sospechosos



Comportamiento y seguimiento

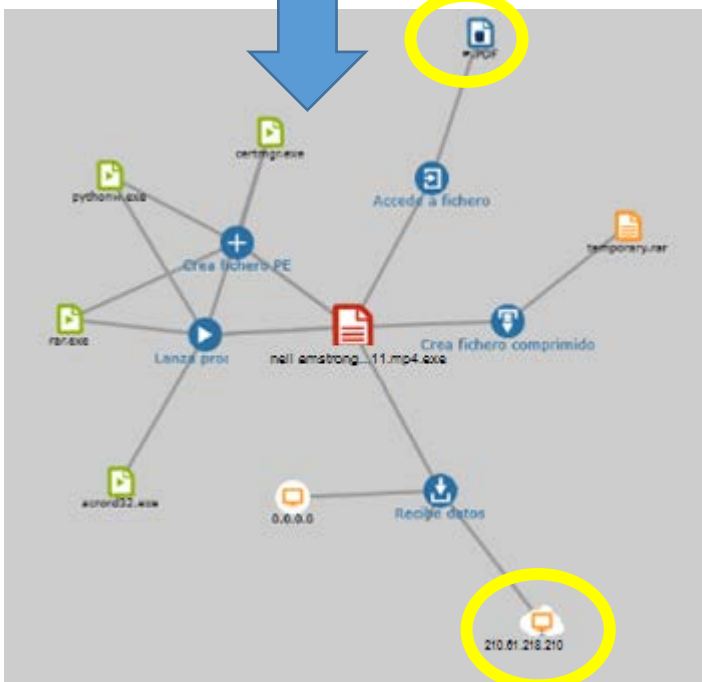
Ruta: MYDOCUMENTS\downloads\neil armstrong transmision original del alunizaje 1969 apolo 11.mp4.exe

Tiempo de exposición: 0 días 0 horas 17 minutos 18 segundos

MD5: 2074D7DB07F1DE881374FBDS

Tecnología de detección: Protección avanzada

Ciclo de vida del malware en el equipo



virustotal

Archivo no encontrado

El archivo que buscas no está en nuestra base de datos.

[Ir a la página principal](#)

[Intentar otra búsqueda](#)

Análisis avanzado



panda OUTGOING NETWORK TRAFFIC USERS ACTIVITY BANDWIDTH CONSUMERS DATA FILE ACCESSED

Map

Destinations of outbound network traffic



machine	machineip	user	hash	driveType	path	protocol	port	direction	dstip
			7A009B9036ECF89AB57011EB615D5E1B	Fixed	WINDOWS\N	TCP	53	Down	221.194.47.20
			7A009B9036ECF89AB57011EB615D5E1B	Fixed	WINDOWS\N	TCP	53	Down	221.194.47.20
			7A009B9036ECF89AB57011EB615D5E1B	Fixed	WINDOWS\N	TCP	53	Down	221.194.47.20
			7A009B9036ECF89AB57011EB615D5E1B	Fixed	WINDOWS\N	TCP	53	Down	221.194.47.20

Analizador CARMEN: desarrollo

Vista General

Nuevo Analizador

Definición

HTTP

DNS

Nombre: TXT-y-TTL-bajo

Descripción: Peticiones DNS de tipo TXT con un TTL bajo

☒ Genera Alerta

Texto de la alerta: Petición DNS TXT con TTL bajo

← Anterior

Siguiente →

Vista General

Nuevo Analizador

Definición

Análisis

+ Dimensiones

Fecha eventoSin función×

IP origenSin función×

+ Condiciones

MaptypeIgual×

TXTY

TTLMenor×

100

+ Parámetros

Por defecto todos los analizadores disponen de un parámetro temporal

← Anterior

Siguiente →

× Cancelar

Analizador CARMEN: ejecución

 TXT-y-TTL-bajo

IP Cliente ▾	Fecha evento ▾
10.49.18.178	30/09/2016 09:59:04.348
10.49.18.176	30/09/2016 11:58:09.599
10.49.18.178	30/09/2016 12:22:57.845
10.49.18.178	30/09/2016 09:49:48.443
10.49.18.176	30/09/2016 11:47:20.348
10.49.18.176	30/09/2016 11:42:10.348
10.49.18.171	30/09/2016 11:42:17.454
10.49.18.178	30/09/2016 12:00:03.548
10.49.18.176	30/09/2016 09:17:27.344
10.49.18.176	30/09/2016 12:11:16.305

Fecha evento ▲	IP origen ▾	Servidor DNS ▾	País ▾	Host ▾	Maptype ▾	IP Respuesta ▾	Respuesta ▾	TTL ▾
30/09/16 09:17:27	✂ 10.49.18.176	192.168.1.22	--	✂ afili.hinet.net	TXT		ouOPrOR0E/Usq3kPpVwCgwd	66
30/09/16 09:49:48	✂ 10.49.18.178	192.168.1.22	--	✂ loak.hinet.net	TXT		2UdUq6A13uQXIMND1BMDr75	34
30/09/16 09:59:04	✂ 10.49.18.178	192.168.1.22	--	✂ loak.hinet.net	TXT		GEEExECACEGCwklBwMCAXUC	87
30/09/16 11:42:10	✂ 10.49.18.176	192.168.1.22	--	✂ loak.hinet.net	TXT		cltC5BbnRvbmIvIFZpbGxhH	56
30/09/16 11:42:17	✂ 10.49.18.171	192.168.1.22	--	✂ loak.hinet.net	TXT		P5r7fGcdWyNzr63LkCDQREa	79
30/09/16 11:47:20	✂ 10.49.18.176	192.168.1.22	--	✂ afili.hinet.net	TXT		2UdUq6A13uQXIMND1BMDr75	48
30/09/16 11:58:09	✂ 10.49.18.176	192.168.1.22	--	✂ loak.hinet.net	TXT		IS6GDOKb6VxUFuwlylDYtZd	52
30/09/16 12:00:03	✂ 10.49.18.178	192.168.1.22	--	✂ loak.hinet.net	TXT		AgAMBQJWE+aGBQKTGytHAAo	30
30/09/16 12:11:16	✂ 10.49.18.176	192.168.1.22	--	✂ loak.hinet.net	TXT		bDseqHHL0RYuQBhGQCP3m3a	41
30/09/16 12:22:57	✂ 10.49.18.178	192.168.1.22	--	✂ loak.hinet.net	TXT		GyMFCRMavZIHcWklBwMadi3	68

Analizador CARMEN: programación

TXT-y-TTL-bajo

Ejecuciones

Configuración

Tags Disponibles

DOMAINS
ANNEX
SENDER
RECEIVER

Tags Configurados

EXFILTRACION
TTL

Guardar

Programación

Lista: Sin selección

Ejecutar cada: 1

A partir de: 30/09/2016

Días

00:00

Desprogramar

Alertas

☒ Generar alerta si la consulta tiene resultados

Guardar

Compartición de IOCs

[Home](#)
[Event Actions](#)
[Input Filters](#)
[Global Actions](#)
[Discussions](#)

MISP

Analistasoc

Log out

[View Event](#)
[View Correlation Graph](#)
[View Event History](#)

[Edit Event](#)
[Delete Event](#)
[Add Attribute](#)
[Add Attachment](#)
[Populate via Freetext Import](#)
[Populate from OpenIOC](#)
[Populate from ThreatConnect](#)

[Delegate Publishing](#)
[Contact Reporter](#)
[Download as...](#)

[List Events](#)
[Add Event](#)

ZeroAccess Campaign 20160930

Event ID

576

Uuid

58074176-d3f4-4770-b149-4668ac130106

Org

S21sec SOC (España)

Contributors

Tags

circ:Incident-classification="malware" x

ms-caro-malware:malware-type="Trojan" x

ZeroAccess x +

Date

2016-09-30

Threat Level

Medium

Analysis

Completed

Distribution

S21Sec MULTISOC

Info

ZeroAccess Campaign 20160930

Published

Yes

Pivots

Attributes

Discussion

= previous

next =

view all

+

Filters: All

File

Network

Financial

Proposal

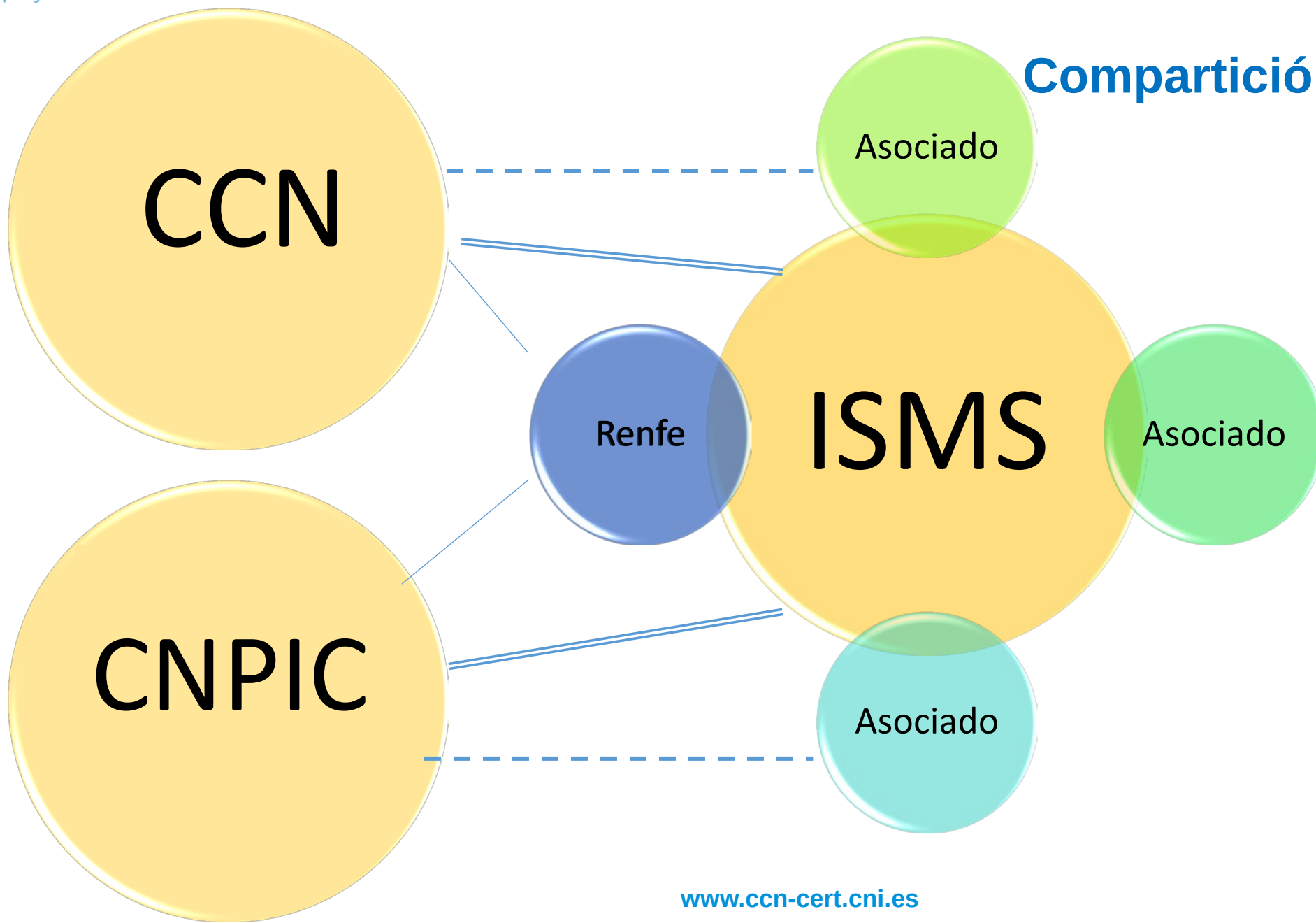
Correlation

Warnings

Include deleted attributes

Date	Org	Category	Type	Value	Comment	Related Events	IDS	Distribution	Actions
2016-09-30		Network activity	domain	i62ka6911.js	Imported via the Freetext Import Tool		Yes	Inherit	
2016-09-30		Network activity	ip-dst	185.25.148.35	Imported via the Freetext Import Tool		Yes	Inherit	
2016-09-30		Network activity	ip-dst	192.185.50.73	Imported via the Freetext Import Tool		Yes	Inherit	
2016-09-30		Network activity	ip-dst	118.163.185.88	Imported via the Freetext Import Tool		Yes	Inherit	
2016-09-30		Network activity	ip-dst	120.29.158.236	Imported via the Freetext Import Tool		Yes	Inherit	

Compartición IOCs ISMS



➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

➤ Síguenos en

